Pay4You Terminal Application (SUM)

Project name	PACT 2
Project number	06937
Title	Pay4You Terminal Application (SUM)
Author	Luc Vermeersch
Version	2.3.0
Status	Release
Classification	Confidential
Info	Saved as *Pay4You_SUM_Terminal*_application_v320.docx, on 2014-04-23 14:59

Project leader:	Date:	Signature:
Manager:	Date:	Signature:

Copyright Statement © 2013 Chess pT B.V

All rights reserved. Disclosure to third parties of this document or any part thereof, or the use of any information contained therein for purposes other than provided for by this document, is not permitted, except with the prior and express written permission of Chess pT B.V.

Document history

Version	Date	Author	Status	Remarks
1.7.4				
	2009-12-15	Wouter Mandemaker	Draft	Added property descriptions, error code descriptions
	2010-01-11	Jacko Brouwer	Draft	Properties to annex, Introduced $5.3.2. Changing parameters
1.7.5	2010-02-03	Werner Dierssen	Draft	Changed NTP client parameters
1.8.0	2010-06-22	Diederik Faber	Draft	Update for TA release 2.2.0
1.9.0	2010-09-14	Jeroen Jensen	Draft	Major additions to section 5.
1.9.1	2010-09-16	Jeroen Jensen	Draft	Major additions to section 5.
1.9.2	2010-09-21	Jeroen Jensen	Draft	Major additions to section 5.
1.9.3	2010-10-25	Jeroen Peterse	Draft	Added C-TAP result codes
1.9.4	2010-11-16	Diederik Faber	Draft	Added property default values, textual enhancements.
1.9.5	2010-12-06	Diederik Faber	Draft	Review comments JENG processed.
1.9.6	2011-03-21	Diederik Faber	Release	Update for TA 2.2.3, review comments JPET
2.0.0	2011-10-05	Diederik Faber	Release	Update for TA 2.3, review comments WMAN
2.0.1	2011-10-06	Jeroen Peterse	Release	Updated magstripetest and transaction result codes
2.1.0	2013-03-20	Luc Vermeersch	Release	Chess pTi style; Update for TA 2.4.0
2.1.1	2013-11-21	Robert Demming	Release	Added ROAS parameters to section **Error! Reference source not found.**. Added RebootReason to section **Error! Reference source not found.**.
2.2.0	2013-11-21	Robert Demming	Release	Update for TA 3.0.0/3.1.0/3.1.1. Added cash register (parameter) description.
2.3.0	2013-11-22	Robert Demming	Draft	Update for TA 3.2.0. Added logo parameters description sections (5.3.9 and 7.1.12).
2.3.1	2014-01-10	Robert Demming	Draft	Update for TA 3.2.0 Added section 5.4.6 and 7.1.13 that describes the new networking switching feature and related parameters. Removed section 5.3.2.5.8.2 (Select Network menu description) since that section is made obsolete by section 5.4.6.
2.3.2	2014-01-24	Robert Demming	Draft	Update for TA 3.2.0 Added section 0 about entering the TMS IP-address from the service menu. Updated section 5.3.1 about entering the TMS IP-address during activation.

Table of contents**1 Scope** 6

1.1 Identification 6
1.2 System overview 6
1.3 Document overview 6
2 Referenced documents 7
3 Software summary 8
3.1 Software application 8
3.2 Software inventory 8
3.3 Software environment 8
3.4 Security and privacy protection 8
3.5 Assistance and problem reporting 8
4 Access to the software 9
4.1 First-time use of the software 9
4.1.1 Equipment familiarization 9
4.1.2 Access control 9
4.1.3 Installation and setup 9
4.2 Initiating a session 9
4.3 Stop and suspend work 10
5 Processing reference guide 12
5.1 Capabilities 12
5.2 Conventions 13
5.3 Processing procedures 13
5.3.1 Activation 13
5.3.2 Main Menu 14
5.3.2.1 Payment 14
5.3.2.2 Reports menu 14
5.3.2.2.1 X Totals 14
5.3.2.2.2 Z Totals 14
5.3.2.2.3 Period Totals 15
5.3.2.3 Paper feed 15
5.3.2.4 Settings menu 15
5.3.2.4.1 Merchant Unit activation 16
5.3.2.4.2 Cash Register activation 16
5.3.2.5 Technical Menu 17
5.3.2.5.1 Test Menu 17
5.3.2.5.2 Service Menu 17
5.3.2.5.3 Terminal Info 17
5.3.2.5.4 Software Info 17
5.3.2.5.5 TSC Info 18
5.3.2.5.6 EMV Info 18
5.3.2.5.7 Management session 18
5.3.2.5.8 Technical Settings menu 18
5.3.2.5.8.1 Restore factory defaults 19
5.3.2.5.8.2 Acquirer messages menu 19
5.3.2.5.8.2.1 Key Load 19
5.3.2.5.8.2.2 Parameter Download 19
5.3.2.5.8.2.3 Open acquirer messages menu 20
5.3.2.5.8.3 Print Card Brand info 20
5.3.2.5.9 Password 20
5.3.2.5.9.1 Change password 21
5.3.2.5.9.2 Forgotten password 21
5.3.2.6 Shutdown 21
5.3.2.7 View last transaction result 21
5.3.2.8 External applications 21
5.3.2.9 Copy receipt 21
5.3.3 Tests 22
5.3.3.1 Auto answer test 22
5.3.3.2 Backlight test 22
5.3.3.3 Battery test 22
5.3.3.4 Buzzer test 22

5.3.3.5 Charge LED test 22
5.3.3.6 Ethernet Test 23
5.3.3.7 File system test 23
5.3.3.8 Keypad test 23
5.3.3.9 Keypad light test 23
5.3.3.10 LCD 23
5.3.3.11 Magstripe test 23
5.3.3.12 Modem test 24
5.3.3.13 Power Button test (On/Off button) 24
5.3.3.14 Power LED test 24
5.3.3.15 Printer test 24
5.3.3.16 RTC test 24
5.3.3.17 Smartcard test 24
5.3.3.18 Soft keys test 24
5.3.3.19 Soft keys light test 25
5.3.3.20 Self-test 25
5.3.3.21 Test report 26
5.3.4 Password authorization 26
5.3.5 Language selection 26
5.3.5.1 Cardholder languages 27
5.3.5.2 Merchant language 27
5.3.6 TIP 27
5.3.7 Payment reference 28
5.3.8 E-Journal 28
5.3.9 Printing Graphical Logo 28
5.4 Related processing 29
5.4.1 Terminal Preparations 29
5.4.2 Low power modes 29
5.4.2.1 Power Save mode 30
5.4.2.2 Low Power mode 30
5.4.2.3 Hibernate 30
5.4.3 Remote management sessions 31
5.4.4 Transaction Data Records (TDR) 31
5.4.5 Software update 31
5.4.6 Network switching 32
5.4.6.1 Introduction 32
5.4.6.2 Network switching modes 33
5.4.6.3 Lost connection detection 33
5.5 Data backup 34
5.6 Recovery from errors, malfunctions, and emergencies 34
5.7 Messages and error codes 35
5.7.1 C-TAP result codes 35
5.7.2 Transaction Host Incident Codes 35
5.7.3 Transaction Result Codes 36
5.7.4 Download Result Codes 36
5.7.5 06 codes 37
5.7.6 Transaction Terminal Treatment Result codes 37
5.8 Quick-reference guide 38
6 Notes 39
7 Annexes 40
7.1 Pay4You Terminal Properties 40
7.1.1 Domain “pact2” 40
7.1.2 Domain “gui” 40
7.1.3 Domain “rdm” 42
7.1.4 Domain “system” 42
7.1.5 Domain “modem” 43
7.1.6 Domain “tdr” 43
7.1.7 Domain “softwareupdate” 43
7.1.8 Domain “tms” 43
7.1.9 Domain “st” 44
7.1.10 Domain “ts” 44
7.1.11 Domain “pact2.ctap” 44
7.1.12 Domain “printer” 47

7.1.13 Domain “network” 47

1 Scope

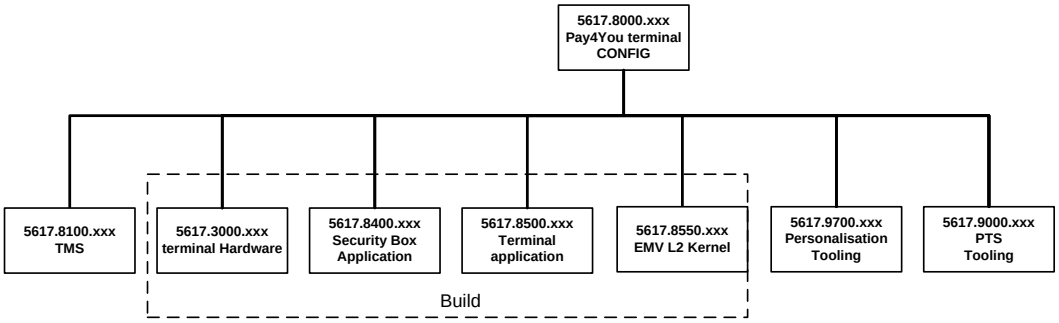
1.1 Identification

This document contains the Software User Manual (SUM) for the Terminal Application version 2.4.0. The Terminal Application is one of the Configuration Items of the Pay4You Terminal manufactured by Chess pTi.

1.2 System overview

Pay4You Terminal is a development by Chess B.V. of a mobile point of sale terminal supporting debit (in Dutch: PIN) and Credit payments, using either chip cards (EMV) or magstripe cards. The terminal conforms to all relevant payment industry and security requirements – PCI, PCI+, EMV level 1, EMV level 2 – to enable its use in the Dutch market according to the Dutch C-TAP specifications and also make it easily adaptable to other European markets.

The complete configuration consists of the following parts:



1.3 Document overview

This document is intended for technical users of the Pay4You terminal. It describes the functionality of the Terminal Application CI offered to the end user, in such a way that software developers and service engineers can operate the terminal. End users are to read [3] for a user manual of the Pay4You terminal.

2 Referenced documents

Ref.	***Description***
[1]	PACT 2 SSDD, version 1.2, November 13th, 2008, Mark Wigmans, Chess B.V.
[2]	Trial-Use Standard, Standard for information Technology, Software Life Cycle Processes Software Development, Acquirer-Supplier Agreement, J-STD-016-1995, *30 September 1995.*
[3]	Installatiegids en gebruikershandleiding Pay4You Terminal, version 3.0, June 24th, 2010, Chess B.V.
[4]	SDD Software Download, version 0.8, march 4, 2010
[5]	C-TAP.200, v3.0, April 2006
[6]	C-TAP Common Parameters 1.8
[7]	Installatiegids en gebruikershandleiding Pay4You MAU, version 0.2, August 27th, 2010
[8]	ROAS - Programmers Guide v1.0
[9]	Pay4You Cash Register Interface - Programmers Guide v1.1

3 Software summary

3.1 Software application

The Terminal Application of the Pay4You terminal comprises all non-secure software parts in the terminal.

Using the Secure Component as a service, the main capability of the Terminal Application software is to perform online payments.

In addition the Terminal Application also has several menus to control the operation of the terminal and a number of menus to test if the hardware and software of the terminal are in expected working order.

3.2 Software inventory

For a listing of all required packages, please refer to the SVD of the current release.

3.3 Software environment

The terminal Application is dedicated software that is specifically designed and written to run on the Pay4You terminal hardware.

The Terminal Application software runs in a Linux environment and is delivered in the form of a distribution. This distribution comes in two forms: as a prebuilt root file system image and as a feed of all packages installed on that root file system. The package manager used by the Terminal Application is IPKG. Besides 'standard' Linux utilities this distribution contains the applications specifically written for the Pay4You terminal.

There is no (server like) software on the terminal that is listening for network traffic, other than terminal initiated communication. This makes the Pay4You terminal suited to be used in a public Internet environment.

To be able to use the terminal in a production environment, the user must have access to a GPRS network. This means a contract with a provider and a SIM card that is to be inserted into the terminal, as well as the necessary contracts with acquirers/banks/etc. to be able to perform live transactions.

3.4 Security and privacy protection

3.5 Assistance and problem reporting

Whenever a problem is detected with the software of the Pay4You terminal, please send a problem report to the Service Manager at Chess pTi:

Lichtfabriekplein 1, 2031 TE Haarlem
T: + 31 (0)85 401 16 40

E: support@chess-pt.com

4 Access to the software

4.1 First-time use of the software

4.1.1 Equipment familiarization

Pressing the small round power button on the left side of the terminal turns on the terminal.

Navigating a menu is done using the three buttons alongside the display. The top and bottom buttons are used to scroll up and down respectively. The middle button is used to select the currently highlighted menu item.

Only when input is requested, the numeric keys can be used.
The STOP key is used to cancel input, or jump to the main menu.
The CORR key is used to erase input, or jump to a higher level menu.
The OK key is used to confirm input, or select the currently highlighted menu item.
The Language key is used to change the language during a payment
The INFO key ('?') is currently not used.

4.1.2 Access control

Most menus and functionality of the terminal are accessible to anyone. The only exception is the TECH SETTINGS menu (Main menu -> Technical menu -> Tech settings), which is secured by a password. Refer to [3] for the value of the password.

4.1.3 Installation and setup

On the first boot of a terminal a menu appears allowing the user to either select the self test menu or start the activation procedure by selecting a network type. The self test is described in detail in **Error! Reference source not found.**. After the activation process is started a unique ID is requested. This ID is used for identification purposes and is therefore under control of the reseller. These IDs are distributed along with the terminal.

The ID has to be entered twice to verify the ID is entered correctly. The terminal automatically starts downloading its configuration from TMS. This can take a few minutes. It may happen that after downloading the configuration a software update may be performed as well (described in 5.4.5). After the configuration is downloaded (or software update process is finished) the main menu is displayed and the user can navigate through the items. The software continues processing all new parameters in the background. This is indicated to the user through messages in the status bar in the top of the display. When the status bar is empty, the terminal is ready and fully operational.

By default the terminal will contact TMS via the URL https://p4ytms:8443/rdm/services/restv1/rdm/. Before starting the installation procedure you have to be sure that p4ytms is redirected by the local network to the correct TMS.

4.2 Initiating a session

Pressing the power button on the side of the terminal turns on the terminal. During the boot phase the screen displays the Pay4You logo. If the terminal has insufficient battery power and no wall adapter is connected, the terminal will beep and an empty battery image is displayed for a few seconds. The terminal will not continue to boot and shut down.

The Pay4You logo is replaced with a start-up message as soon as the low-level system software is initialized and the application software is started.

The main menu is displayed when the terminal software is started up. At this point most of the functionality of the terminal is ready for use. The payment functionality takes some time longer to initialize. This is indicated in the status bar as 'INITIALIZING x/6'. When the status bar is empty, the terminal is fully operational.

The status bar may give other information as well. Below is a table of all messages displayed, what they mean and how to remedy them. The status bar messages are language dependant, this table shows the English texts.

Status bar message	Cause	Remedy
'INITIALIZING x/6'	The payment software is initializing (split in six phases)	Wait for payment software to become ready.
'CHECK PRINTER'	Something prevents tickets to be printed. Probably there is no paper or the printer lid is not closed correctly.	Check printer paper and close lid properly.
'CHECK BATTERIJ'	The battery is near empty.	Attach power cable.
'CHECK NETWORK'	The terminal could not establish a network connection	Depending on network type, check the Ethernet cable or check if the sim card is inserted properly.
'PLEASE WAIT'	The terminal is performing some background task that temporarily prevents payments to be performed.	Wait for background task to finish.
'REINITIALIZE'	The terminal is reinitializing after a remote management session.	Wait for the initialization to finish.
'CONFIGURATION ERROR (n)'	The payment software is missing mandatory parameters. Payments are not possible.	The n indicates the error. Configure the terminal properly. Make sure the correct configuration is loaded in TMS and start a management call. Or, go back to factory settings. (1) Common parameters error (2) Terminal Manager parameters error (3) Date for update error (4) Cert.Code error (5) Terminal Manager error (6) Terminal Manufacturer error (7) No valid acquirers (8) Terminal Model error (9) CAPK parameters error (10) Terminal country code error (11) Terminal type error (12) Access provider error (13) Interface device serial number error
'OUT OF ORDER'	The payment software is missing mandatory parameters. Payments are not possible.	Configure the terminal properly (check if card brands are set up correctly). Make sure the correct configuration is loaded in TMS and start a management call. Or, go back to factory settings.

4.3 Stop and suspend work

There are four ways to shut down the terminal:

1. Select the shutdown option from the main menu
2. Press the Power button and confirm the shutdown using the soft keys
3. Press the Power button and hold for 5 seconds.
4. Low power mode

Option 1 and 2 provide proper shut down functionality. The display is turned off within seconds, but the red power led stays lit for some time longer (up to a minute). During this time the terminal goes into so called suspend-to-flash mode, which allows for faster boot times when the terminal is turned on again.
The terminal is completely powered off when the red power led is turned off.

Option 3 should not be used other than as a last resort. It kills power to the system abruptly, which may eventually lead to file system corruption or physical damage to the display.

Option 4 will bring the terminal in sleep mode. The terminal will start-up within seconds. See section 5.3.5.

5 Processing reference guide

5.1 Capabilities

The user can operate the terminal by selecting options from the menu. A full menu map is shown here. Note that the labels change when a different language is selected:

- PAYMENT
- REPORTS
  - X TOTALS
  - Z TOTALS
  - PERIOD TOTALS
    - CLOSE
    - PRINT
      - CURRENT
      - CURRENT/PREV.
      - PREVIOUS
- PAPER FEED
- SETTINGS
  - LANGUAGE
  - CONTRAST
  - DISPLAY LIGHT
  - KEYPAD LIGHT
  - MERCHANT UNIT
  - CASH REGISTER
  - SWITCH NETWRK (only when terminal has modem and is enabled in TMS)
- TECHNICAL MENU
  - TEST MENU
    - ALL TESTS
    - PRINT RESULTS
    - AUTOANSWER
    - BACKLIGHT
    - BATTERY
    - BUZZER
    - CHARGE LED
    - ETHERNET
    - FILE SYSTEM
    - KEYPAD
    - KEYPAD LIGHT
    - LCD
    - MAGSTRIPE
    - MODEM
    - ON/OFF BUTTON
    - POWER LED
    - PRINTER
    - RTC
    - SMARTCARD
    - SOFTKEYS
    - SOFTKEYS LIGHT
    - SOFTWARE INFO
  - SERVICE MENU (password protected)
    - CLEAN SWEEP
    - BLOCK PAYMENT
  - TERMINAL INFO
  - TSC INFO
  - EMV INFO
  - SOFTWARE INFO
  - UPDATE
  - SOFTWARE UPDATE
  - TECH SETTINGS (password protected)
    - FACTORY RESET

- SELECT NETWORK (only when terminal has modem and is enabled)
- ACQ. MESSAGES
  - OPEN MESSAGES
    - SHOW MSG
    - SEND ADVICE
  - KEYLOAD
  - PARAM DWNLD
- CARDBRAND INFO

- PASSWORD
  - CHANGE
  - FORGOTTEN

- SHUTDOWN
- LAST TRANS.
- ADDED FUNCT.
- COPY RECEIPT

5.2 Conventions

During menu navigation, the STOP key always returns to the 'PAYMENT' option in the main menu. The CORR key jumps up one level in the menu hierarchy.

5.3 Processing procedures

The functional blocks of the terminal are described in the following paragraphs. This paragraph focuses on the functions a user can trigger from the menu. Paragraph 5.4 explains all the processes that operate in the background.

5.3.1 Activation

The activation involves the following steps:

1. Selecting network type
2. Entering the activation code
3. Entering the activation code again
4. Performing Configuration Management session

The interface selection menu shows the following options.

- The possible network types that the terminal supports. (ETHERNET / GPRS)
- Option to enter the Test Menu (SELFTEST), see paragraph 5.3.2.5.1.

At step 2 and 3, an 11 proof activation code needs to be entered. This code is supplied as part of the terminal. When the code entered is not 11-proof an error message is shown. When the codes entered are not the same, another error message is shown.

During step 4, the terminal tries to retrieve its configuration from the TMS through a remote management session. See 5.4.3 for future details. The management session is restarted until is succeeds.

Since terminal software release 3.2, it is also possible to enter the IP-address / port number of the TMS server during activation. This is useful if the terminal is connected to a network where the default TMS host name (https://p4ytms:8443) is not configured in the DNS. When the TMS cannot be reached, the activation procedure will give the opportunity to enter the TMS IP-address again. See section 0 (Change TMS) for more information about entering the IP address.

Note: Activation must always be done over Ethernet since GPRS is not configured until a management session is done.

5.3.2 Main Menu

The main menu contains the following options:

- Option to start a payment (PAYMENT), see paragraph 5.3.2.1.
- Option to enter the reports menu (REPORTS), see paragraph 5.3.2.2.
- Option to execute a paper feed (PAPER FEED), see paragraph 5.3.2.3.
- Option to enter the settings menu (SETTINGS), see paragraph 5.3.2.4.
- Option to enter the technical menu (TECHNICAL MENU), see paragraph 5.3.2.5.
- Option to execute the shutdown processing (SHUTDOWN), see paragraph 5.3.2.6.
- Option to view the result of the latest transaction (LAST TRANS.), see paragraph 5.3.2.7.
- Option to select an external application (ADDED FUNCT.), see paragraph 5.3.2.8.
- Option to print a copy ticket (COPY RECEIPT), see paragraph 5.3.2.9.

5.3.2.1 Payment

This option starts a sale transaction. Depending on the configuration of the terminal cards (magstripe/EMV) will be accepted or refused. Also the transaction flow depends on the configuration (reference data, user guidance 1 or 2, tip entry).

See [3] for more details.

5.3.2.2 Reports menu

The report menu contains the following options:

- Option to print the X Totals (X TOTALEN).
- Option to print the Z Totals (Z TOTALEN).
- Option to print the period totals (PERIODE TOTALEN).

5.3.2.2.1 X Totals

During the processing of the X Totals, the X Totals report is printed. The X Totals report contains the totals since the last moment the X/Z totals are cleared. See Z totals for clearing the X/Z totals.

The X Totals report contains the following information:

- The period number
- Date and time since the last moment the totals were cleared
- The current date and time
- For each acquirer
    - The terminal ID (KASSNR)
    - The name of the acquirer
    - For each card brand couple to this acquirer
        - The name of the card brand
        - The number of transaction performed with this card brand per service type
        - The total amount performed with this card brand per service type
- Overall number of transactions
- Overall amount

5.3.2.2.2 Z Totals

During the processing of the Z Totals, the Z Totals report is printed. The Z Totals report contains the totals since the last moment the X/Z totals are cleared. Printing the Z Totals clears the X/Z totals.

The Z Totals report contains the same information as part of the X Totals. See X Totals processing for details.

5.3.2.2.3 Period Totals

During the first step of the Period Totals processing, the user is asked whether:

- The period needs to be closed
- The period needs to be printed.

When the period needs to be closed, the terminal closes the current period with each active acquirer. After the period is closed, the terminal prints the previous and current totals. Closing the periods manually only works when supported by the acquirer!

When the periods need to be printed, the user is asked which period needs to be printed. The options are:

- Current period
- Previous and current
- Previous period

When a selection is made the terminal starts downloading the appropriate period counters from each acquirer and the prints the receipt.

The period report contains the following information:

- A header
- Which types of periods are being reported
- The current date and time
- For each acquirer
    - The name of the acquirer
    - The terminal id of the terminal as known by the acquirer (KASSNR)
    - For each counter
        - The ID of the counter and the currency of the counter
        - The type of the counter
        - The brand of the counter
        - The service type of the counter
        - For each period
            - The period number
            - Start time and date
            - Stop time and date
            - Number of transaction
            - The total amount of the transaction.

5.3.2.3 Paper feed

Scrolls the printer paper.

5.3.2.4 Settings menu

The settings menu is entered by selecting “SETTINGS” from the main menu.
The menu contains the following options:

- Language selection, see paragraph 5.3.5.
- Change the display’s contrast (CONTRAST), select + for a higher contrast or – for a lower contrast.
- Enable the display backlight (DISPLAY LIGHT), select ON to enable or OFF to disable.
- Enable/disable the keypad lighting (KEYPAD LIGHT), select ON to enable or OFF to disable.
- Activate the MERCHANT UNIT, select YES to activate, NO to cancel activation (see section 5.3.2.4.1).

- Activate the cash register interface, select YES to activate, NO to cancel activation (see section 5.3.2.4.2).
- Switch the active network temporary, does not switch the preferred network. This option is only available when the terminal supports multiple network types and network switching is enabled. For more information see section 5.4.6.

5.3.2.4.1 Merchant Unit activation

Merchant Unit activation can be activated from the Settings Menu.

Before the merchant unit is activated, the user needs to confirm this. When the user confirms, the terminal tries to activate the Merchant Unit. When the activation succeeds, the terminal enters the Merchant Unit mode and starts waiting for amounts entered on the Merchant Unit.

The processing in relation to the Merchant Unit is described in the Merchant Unit SUM. See [7].

5.3.2.4.2 Cash Register activation

A cash register connection can be activated from the Settings menu. Before the cash register connection is activated, the user needs to confirm this. When the user confirms, the terminal tries to contact the cash register that is specified in the cash register parameters. When the connection succeeds, the terminal enter cash register mode and waits for commands from the connected cash register.

The cash register connection can be deactivated by a command from the cash register or by pressing the power button shortly and accepting the confirmation question.

The cash register to connect to is specified by the “gui:CashRegister.ConnectionString” parameter. Its general format is:

```
<protocol>#<medium>;<communication parameters>
```

The supported protocol is currently only “ProtoBuf” (Google protocol buffers). In future version other protocols might be supported. When the protocol (and #) is left out, “ProtoBuf” is assumed. The only supported medium is currently “TCP” but in future versions other mediums like “SERIAL” or “USB” could be supported. When the medium (and ;) is left out, “TCP” is assumed. The communication parameters are depending on the medium and are separated by colons (:). For TCP the communication parameters are:

```
<host>:<port>
```

When port is not given, port 10000 is used. Some example connection strings:

```
ProtoBuf#TCP;pc-pti-100.chess.nl:10000     // Protobuf protocol over TCP
                                           // with host name + port number.
TCP;172.17.100.21:10000          // Protobuf protocol (implicit) over TCP
                                 // with IP address + port number.
pc-pti-100                       // Protobuf protocol (implicit) over TCP (implicit)
                                 // with host name on the default port.
```

The “gui:CashRegister.Message” parameter determines the message to show on the terminal while it is waiting for commands from the cash register.

The “gui:CashRegister.KeepAliveInterval” specifies the time between keep-alive message sent from the terminal to the cash register. This is used to detect when the connection is broken e.g. when the cable is detached. Don’t make it too small else a keep-alive time-out could be generated when the terminal is very busy. Don’t make it too long else a cable detachment will take a long time to detect. Values between 10 and 60 seconds seem appropriate.

Finally the “gui:CashRegister.Status” determines if the cash register interface is “disabled” (0), “enabled” (1) or “active” (2). When enabled, the terminal will automatically try to connect to the cash register when it starts up. When a connection is made, the status will be “active”. The terminal will set/change this parameter thus do not set it with TMS.

5.3.2.5 Technical Menu

The technical menu can be entered by selection option “TECHNICAL MENU” from the main menu.

The menu contains the following options:

- Option to enter the test menu (TEST MENU).
- Option to enter the service menu (SERVICE MENU).
- Option to execute the terminal info processing (TERMINAL INFO).
- Option to view the TSC info (TSC INFO).
- Option to view the EMV info (EMV INFO).
- Option to execute the Software Info processing (SOFTWARE INFO).
- Option to initiate Terminal Application Software update (SOFT. UPDATE).
- Option to initiate a management session (UPDATE).
- Option to enter the technical settings menu (TECH SETTINGS).
- Option to execute the password processing (PASSWORD).

5.3.2.5.1 Test Menu

The test menu can be entered from:

- Selecting the option “SELFTEST” from the initial interface selection menu.
- Selecting the option “TEST MENU” from the Technical Menu.

The Test Menu contains:

- The option “ALL TESTS” to executes the self test.
- The option “PRINT RESULTS” to print the test results report.
- Options to perform all possible tests individually. Tests, depending on capabilities that are not supported by the terminal configuration, are not shown.
- The option “SOFTWARE INFO” to execute the Software Info processing.

After each test started from the Test Menu, the user is asked to repeat the test or not.
Returning to the Test Menu after a test differs from all other menus. The last performed is selected again instead of the first option. For details about the specific tests see 5.3.3.

5.3.2.5.2 Service Menu

This menu is only accessible for service personnel

5.3.2.5.3 Terminal Info

This processing procedure can be activated from the Technical Menu.

During this procedure the following screens are shown:

- Information screen indicating the activation code of the terminal.
- Information screen indicating the Ethernet IP address of the terminal.
- Information screen indicating the GPRS IP address of the terminal.
- Information screen indicating the Terminal Serial Number of the terminal.
- Information screen indicating the Domain of the terminal
- Information screen indicating the current time as known by the terminal

The user is indicated to press the OK key to jump to the next screen.

5.3.2.5.4 Software Info

The Software Info processing can be activated from the Technical Menu and from the Test Menu.

During the processing of the Software Info, the terminal prints the packages list of the terminal. The package list contains for each software packages the currently installed version.

5.3.2.5.5 TSC Info

The TSC Info processing can be activated from the Technical Menu.

During the processing the terminal shows an information screen containing the following data:

- TSC manufacture ID. (MF ID: 5280008)
- Security Box Serial Number (or TSC Serial Number) (SB SN)
- Secure Component (or TSC) Version Number (SC SV)

The only way to leave the information screen is by pressing the OK key. This screen differs from the normal convention.

5.3.2.5.6 EMV Info

The EMV Info processing can be activated from the Technical Menu.

During the processing the terminal shows information screen containing the following data:

- EMV Kernel Checksum

5.3.2.5.7 Management session

The Management session processing can be activated from the Technical Menu.

During the management session processing the following steps are executed:

1. The terminal asks for confirmation. When the user does not confirm the processing is aborted.
2. The terminal requests the management call. During this step, the user can abort the processing by pressing the STOP key.
3. The terminal performs the management call. See paragraph 5.4.3 for details.
4. The properties are updated.

After the processing, the terminal returns to the Technical Menu. Next the terminal will reinitialize itself.

When the management call fails at step 3, the terminal shows a failure screen.

5.3.2.5.8 Technical Settings menu

The processing of the technical settings menu can be activated from the Technical Menu.

Before the menu is shown, the password authorization processing is executed. Only when this processing is successful the menu is shown, otherwise the technical settings menu processing is aborted.

The menu contains the following options:

- Restore the factory default (FACTORY RESET).
- Select the preferred network type (SELECT NETWORK). This option is only available when the terminal supports multiple network types and network switching is enabled. For more information see section 5.4.6.
- Acquirer messages menu (ACQ. MESSAGES).
- Print the Card Brand info (CARDBRAND INFO).

5.3.2.5.8.1 Restore factory defaults

Restoring the factory defaults can be activated from the Technical Settings Menu.

Before the factory defaults are restored, the user needs to confirm this.
When the user does not confirm the processing is aborted.

When the user confirms to restore the factory defaults, the terminal request from the TMS the factory defaults. See paragraph 5.4.3 for details.

Please note: The defaults of the terminal might differ from the factory default from the TMS.
Restoring factory defaults is implemented from an “end user” point of view and not from a “service engineering” point of view.

5.3.2.5.8.2 Acquirer messages menu

The processing of the acquirer message menu can be activated from the Technical Settings Menu.

The menu shows the following options:

- Option to execute the Key Load processing (KEYLOAD).
- Option to enter the Parameter Download processing (PARAM DWNLD).
- Option to enter the Open messages menu (OPEN BERICHTEN).

5.3.2.5.8.2.1 Key Load

The key load processing can be activated from the acquirer messages menu.

First the terminal asks to select a Security Provider to perform the key load from. The list contains the Security Provider Identifiers as specified in the C-TAP Common Parameters [6].

When the Security Provider is selected, the terminal will initiate a key load for the given Security Provider. After the Scheme Load is performed, the terminal will perform Parameter Updates related acquirers.

See paragraph for 5.7.4 for error codes description indicating the reason of failed key loads.

During normal use this functionality is not needed. When a key load is needed, the terminal will automatically do this. This functionality is only needed for error recovering and during the certification of the terminal.

5.3.2.5.8.2.2 Parameter Download

The parameter download processing can be activated from the acquirer messages menu.

First the terminal asks to select a Acquirer to perform the parameter download from. The list contains the acquirer Identifiers or the acquirer labels of the acquirer specified in the Common Parameters. The identifier is shown when the label is known (since it is specified by the Acquirer).

When the acquirer is selected, the terminal will initiate a parameter download from for the given acquirer.

See paragraph for 5.7.4 for error codes description indicating the reason of failed parameter downloads.

During normal use this functionality is not needed. In normal use, the parameter downloads are automatically done. This functionality is only needed during error recovery and the certification of the terminal.

5.3.2.5.8.2.3 Open acquirer messages menu

The processing of the open acquirer message menu can be activated from the Acquirer message menu.

The menu shows the following options:

- Option to view an open acquirer messages (TONEN MSG).
- Option to send an open acquirer messages (VERZEND ADVIES).

5.3.2.5.8.2.3.1 View open acquirer messages

From the open acquirer messages menu, the 'view open acquirer message' can be activated.

The terminal shows a list of open message to be sent to a acquirer.

During normal use this functionality is not needed.

5.3.2.5.8.2.3.2 Send open acquirer messages

From the open acquire message menu, see paragraph 5.3.2.5.8.2.3, the send open acquirer message processing can be activated.

The terminal shows a menu with the open message to be sent to an acquirer. When a message is selected, the terminal tries to send the message to the host.

During normal use this functionality is not needed since message are automatically sent to the acquirer.

5.3.2.5.8.3 Print Card Brand info

Printing the card brand info can be activated from the Technical Settings Menu.

The receipt contains the card brand info split up in card brands coupled with an acquirer and brands without an acquirer.
The receipt contains for each acquirer:

- The name of the acquirer
- The ID of the terminal; how the terminal is known to the acquirer. (KASSNR).
- For each card brand that is coupled to the given acquirer
    - The name of the card brand
    - The Merchant User Identifier used for the given card brand (Winkelier ID)

The Account numbers (Rekening(en)) configured for the given card brand.

5.3.2.5.9 Password

This processing can be activated from the Technical Menu.

The password processing contains two sub processing, namely:

- Processing to change the password
- Processing to handle a forgotten password

The above sub processing can be activated through the menu. When the option CHANGE is selected, the processing to change the password is executed. When the option FORGOTTEN is selected, the processing to handle a forgotten password is executed.

5.3.2.5.9.1 Change password

From the Password processing, the processing to change the password can be activated.

Changing the password involves the following steps:

1. The terminal asks executes the Password Authorization processing. See paragraph 5.3.4
2. The terminal asks for the new password (number)
3. The terminal asks to enter the new password again.

After step 3, the password has been changed (and stored to the designated property) and the terminal returns to the Password processing.

When the Password Authorization fails at step 1, the Change the password is aborted at step 1. When the passwords entered at step 2 and 3 are not the same, the terminal shows a failure screen before returning to the Password processing.

5.3.2.5.9.2 Forgotten password

From the Password processing, the processing to change the password can be activated.

A custom message screen is shown to the user to indicate what to do. By default, this instructs the user to contact the Service Provider of the terminal.

5.3.2.6 Shutdown

After selecting Shutdown in the main menu, the action needs to be confirmed with YES to shutdown or NO if you wish not to shutdown the terminal and return to the main menu. After selecting YES, the display is turned off within seconds, but the red power led stays lit for some time longer (up to a minute).
During this time the terminal goes into so called suspend-to-flash mode, which allows for faster boot times when the terminal is turned on again by the power button. The terminal is completely powered off when the red power led is turned off.

See [3] for more details.

5.3.2.7 View last transaction result

Shows the results and the date and time of the last transaction.

5.3.2.8 External applications

Present a list of registered external applications. See [8] for details about ROAS.

5.3.2.9 Copy receipt

Reprints the receipt of the last transaction, if available.

5.3.3 Tests

The terminal is able to perform tests to verify whether the terminal is functioning correctly. The following describes:

- The processing of the individual tests. Paragraph 5.3.3.1 through 5.3.3.19.
- The self-test, paragraph **Error! Reference source not found.**.
- The test report, paragraph 5.3.3.21.

In general, the following conventions apply to all tests:

- All user confirmation screens support a timeout. When a confirmation times out, the test is considered inconclusive.

5.3.3.1 Auto answer test

Sets the GPRS modem in auto answer mode. When this mode is activated, the GPRS modem will answer calls automatically. This is useful functionality for testing the modem during production. This test is only available when the terminal has GPRS capabilities.

5.3.3.2 Backlight test

Steps:

1. The backlight is toggled.
2. The terminal asks the user to confirm that the backlight did go on and off.

The test passes when the uses confirms question at step 2.

5.3.3.3 Battery test

Steps:

1. Measures and shows the battery voltages.

When the battery voltage is between expected values, the test passes. The battery voltages should be between 7200 and 8500 mV.

This test is only available when the terminal has the battery capability.

5.3.3.4 Buzzer test

Steps:

1. The terminal makes three sounds
2. The terminal asks the user to confirm that three sounds where hearable.

The test passes when the uses confirms question at step 2.

5.3.3.5 Charge LED test

Steps:

1. The terminal indicates to:
    - Disconnect the power cable
    - Connect the power cable
    - To press a soft keys
2. The terminal indicates the user to confirm that the upper orange LED (Charge LED) is on

The test passes when the uses confirms question at step 2.

This test is only available when the terminal has the battery capability.

5.3.3.6 Ethernet Test

Steps:
1. The terminal shows the IP address of the Ethernet interface.

The test passes when the terminals has a IP address for the Ethernet interface

5.3.3.7 File system test

Steps:
1. The terminal shows how much disk space is used.

5.3.3.8 Keypad test

1. The terminal indicates the user to press:
   - Language button
   - Info key (?) button
   - STOP key button
   - CORR key button
   - OK key button
2. The terminal indicates the user to enter:
   - 1234567890

The test passes when the key presses are successfully retrieved.

5.3.3.9 Keypad light test

Steps:
1. The keypad light is toggled.
2. The terminal asks the user to confirm that the keypad light did go on and off.

The test passes when the uses confirms question at step 2.

5.3.3.10 LCD

Steps:
1. The terminal shows a black screen
2. The terminal asks the user to confirm that all the pixels are ok.

The test passes when the uses confirms question at step 2.

5.3.3.11 Magstripe test

Steps:
1. The terminal asks the user to swipe a magstripe card

The test passes when all 3 tracks of the magstripe data are read. The test fails when no tracks are read. The test is inconclusive when 1 or 2 tracks are read. This all depends on the card used during this test

5.3.3.12 Modem test

Steps:
1. The terminal shows the signal strength

This test is only available when the terminal has the battery capability.

5.3.3.13 Power Button test (On/Off button)

Steps:
1. The terminal asks the user to press the power button.

The test passes when the power button press is retrieved.

5.3.3.14 Power LED test

Steps:
1. The terminal asks the user whether the power led is on.

The test passes when the uses confirms question at step 1.

5.3.3.15 Printer test

Steps:
1. The terminal prints text.
2. The terminal asks the user whether the terminal printed text.

The test passes when the uses confirms question at step 2.

5.3.3.16 RTC test

Steps:
1. The terminal shows the data and time retrieved from the RTC (Real Time Clock).

5.3.3.17 Smartcard test

Steps:
1. The terminal asks the user to insert a smart card.
2. The terminal asks the user to remove the smart card

The test passes when step 1 and step 2 are correctly detected and when initialization of the smart card succeeded at step 1.

5.3.3.18 Soft keys test

Steps:

1. The terminal asks the user to press the upper soft key
2. The terminal asks the user to press the middle soft key
3. The terminal asks the user to press the lower soft key

The test passes when the terminal retrieves all soft keys presses in order.

5.3.3.19 Soft keys light test

Steps:
1. The terminal turns all lights of (expect for power and charge LEDs)
2. The terminal toggles the soft key lights
3. The terminal restores all lights.
4. The terminal asks the user to confirm whether the soft key light turned on and off.

The test passes when the user confirms the question at step 4.

5.3.3.20 Self-test

The terminal is able to perform a self-test to verify the whether the hardware of the terminal is correctly functioning. The self-test is designed to be used during the:
- Outgoing quality checks (OQC)
- Incoming quality checks (IQC)
- Normal use

The self-test can be active by:
- Selecting the option “ALL TESTS” from the Test Menu. See 5.3.2.5.1.

The following tests are performed as part of the self-test:
- Backlight test, see paragraph 5.3.3.2.
- Battery test (only when the terminal config contains a battery), see paragraph 5.3.3.3.
- Buzzer test, see paragraph 5.3.3.4.
- Charge LED test (only when the terminal config contains a battery), see paragraph 5.3.3.5.
- Keypad test, see paragraph 5.3.3.8.
- Keypad light test, see paragraph 5.3.3.9.
- LCD test, see paragraph 5.3.3.10.
- Magstripe test, see paragraph 5.3.3.11.
- Power button test, see paragraph 5.3.3.13.
- Power LED test, see paragraph 5.3.3.14.
- Printer test, see paragraph 5.3.3.15.
- Smart card test, see paragraph 5.3.3.17.
- Soft keys test, see paragraph 5.3.3.18.
- Soft keys light test, see paragraph 5.3.3.19.

When a test fails, the user is asked whether the user wants to repeat the test.

After the above tests are performed, the terminal shows the test result summary. Possible results are:
- PASSED
  All tests are passed
- FAILED
  One or more tests are failed.
- INCONCLUSIVE
  One or more tests are inconclusive

Next, the terminal asks the use whether a test reports should be printed. When the option is confirmed, the test report is printed. See After printing the test result or when printing the report is skipped, the terminal returns to the previous processing (Activation or Test menu).

The following tests are not part of the self-test:

- Ethernet test, see paragraph 5.3.3.6.
- File system test, see paragraph 5.3.3.7.
- Modem test, see paragraph 5.3.3.12.
- RTC (Real Time Clock) test, see paragraph 5.3.3.16.

The Ethernet test and modem test are not performed as part of the self-test since they depend upon external system facilities. The File System and RTC clock are not performed as part of the self-test since the test result is ambiguous.

5.3.3.21 Test report

The test report contains the following sections:

- Header
  - Terminal Serial Nr
    The serial number of the terminal.
  - The serial numbers for each Printed Circuit Assembly (PCA) inside the terminal.
    - KPC PCA Serial Nr
    - PowerIO PCA Serial Nr
    - LCD PCA Serial Nr
  - Terminal Product ID
  - TSC (Terminal Secure Component) Serial Nr
  - TSC (Terminal Secure Component) Software version number
  - CPLD Firmware version
    The firmware version of the CPLD (Complex Programmable Logical Device.
  - Pact2live Version
    The software version of the Terminal Application.
  - Pact2live VM Version
    The software version of the Linux kernel
- The test results
  - The results of the tests performed during the self-test.
  - The results of other tests not part of the self-test.
- Summary
  - The overall test results. PASSED, FAILED or INCONCLUSIVE
  - The amount of tests passed
  - The amount of tests failed
  - The amount of tests inconclusive

The test report can be printed as part of the self-test (see paragraph **Error! Reference source not found.**) and can be printed from the Test Menu (see paragraph 5.3.2.5.1).

5.3.4 Password authorization

The password authorization processing asks the user to enter a password (number). The password is verified against the property containing the password. When the password verification is successfully, the processing returns with a success code, otherwise message screen indicating the password failure is shown. After pressing the OK key, the processing returns a failure code.

The entered numbers are visible during the password entering. This is required by the specification. Only PIN codes are allowed to be entered with * signs.

5.3.5 Language selection

The terminal has two distinct models of multi-language support: one for the merchant and one for the cardholder.

5.3.5.1 Cardholder languages

The terminal supports four languages for the cardholder: Dutch, English, German and French. These languages are specified by CTAP.

The default cardholder language to use during a transaction is configured by the property pact2.ctap:language. Possible values are “DUTCH”, “ENGLISH”, “GERMAN” and “FRENCH”.

When the swiped or inserted card contains language information, the terminal will automatically switch to that language.

The cardholder can change the language during a transaction by pressing the language button. Pressing the language key multiple times cycles through the available languages

5.3.5.2 Merchant language

The terminal software supports a number of languages for the merchant. Currently these are Dutch, English, German and French, but other languages may be added in the future.

Although all available languages are installed on the terminal, it is configurable through TMS which languages can be selected by the user. To this end the property gui:AllowedMerchantLanguages is available.
The format of this property is a space or comma separated list of <locale>:<label> values. The <locale> designates the locale to use on the terminal, thereby selecting the language as well. The <label> is shown in the Language Selection menu.

The cross section of the installed languages on the terminal and the configured allowed languages make up the entries in the Language Selection menu.

For example, if the languages Dutch, English, German and French are installed on the terminal and the property gui:AllowedMerchantLanguages is configured as “nl_NL:NEDERLANDS en_US:ENGLISH pl_PL:POLSKI”, then the language selection menu will display the two entries NEDERLANDS and ENGLISH.

The current selected language (locale) is reflected in the property gui:MerchantLocale. The value of this property can be changed through the language selection menu on the terminal or via TMS.

5.3.6 TIP

In order for the tip functionality to work, the following properties need to be configured correctly on the terminal (see 5.4.3 for a description on how to do that). If any property is missing or not set, the tip functionality is not available. By default tip is disabled.

Domain	Name	Description
pact2.ctap	tipEnabled	Set to 1 to enable tip functionality, 0 to disable.
pact2.ctap	maxTipAllowed	0 < value < 100 (both exclusive). If 0, no tip is possible because the tip amount is 0,00. Max value is 99, because the tip is not allowed to be equal to or more than the transaction amount.
st	request.tip.nl	Dutch secured text for tip entry screen.
st	request.tip.de	German secured text for tip entry screen.
st	request.tip.en	English secured text for tip entry screen.
st	request.tip.fr	French secured text for tip entry screen.
ts	request.tip.nl	Signature for Dutch tip entry text.
ts	request.tip.de	Signature for German tip entry text.
ts	request.tip.en	Signature for English tip entry text.
ts	request.tip.fr	Signature for French tip entry text.

Tip functionality is only supported for user guidance 1. For user guidance and a functional description on how tips are entered, please refer to [3].

NB: Tip also needs to be enabled by the acquirer on the merchant contract!

5.3.7 Payment reference

The payment reference functionality is enabled by setting the property gui:paymentReferenceEnabled to 1. If set to 0, the payment reference functionality will not be executed.

It is possible to configure a payment reference prefix using the property gui:PaymentReferencePrefix. This prefix is printed on the receipt in front of the entered reference

For a functional description on how payment references are entered, please refer to [3].

5.3.8 E-Journal

The e-journal functionality is enabled if the pact2.ctap:eJournalEnabled property is set to 1. If enabled, the terminal will send an electronic record of each transaction to TMS.

If e-journals are enabled, the merchant can choose whether the journal ticket is to be printed or not, by configuring the property pact2.ctap:printTxnJournal. If set to 1, the journal ticket is printed. If set to 0, it is not printed.

Note that if e-journal functionality is disabled, the property pact2.ctap:printTxnJournal is ignored and the journal ticket is always printed.

5.3.9 Printing Graphical Logo

Since terminal software version 3.2 it is possible to print a graphical logo on the card holder ticket. The parameter “printer:GraphicalLogo.Enable” determines if a logo (if available) is printed at the top of the ticket.

The parameter “printer:GraphicalLogo.BitmapData” is used to transfer the logo bitmap to the terminal. The bitmap data must be a monochrome .bmp file that is base64 encoded. There are various tools to convert a file to base64 encoded data. One online example is: http://www.opinionatedgeek.com/dotnet/tools/base64encode/

The width of the bitmap can be maximum 384 pixels wide. The base64 encoded bitmap can optionally be prepended by a description between square brackets. An example of the bitmap data parameter is (a star shaped logo of 32x32 pixels):

```
[SmallStar.bmp]Qk2+AAAAAAAAAD4AAAAoAAAAIAAAACAAAAABAAEAAAAAAIAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAP///wD9//+//P//P/4//H/+H/h//gfgf/4DwH//AYD//wAA//8AAP//gAH//4AB//+Aaf//gAH
//wAA//4AAH/8AAA/8AAAD+AAAfAAAADAAAAAP/AA///8A////gf///4H///+B////w////8P////D////
w////+f////n////5//w==
```

During a management session, the bitmap is uploaded to the terminal and save locally to “/usr/share/bitmaps/logo.bmp”. Then the bitmap data parameter is cleared except for the description. It takes another management session to update this also in TMS. The bitmap data is removed from the parameter because the data can be relatively large and we don’t want to transfer that when a full parameter exchange is done.

Because of limitations of the terminal’s printer it is advised the limit the number of black pixels to 128 per line. When a line contains more than 128 pixels, the printing process takes longer and the quality decreases. Thus avoid logos with large black areas. Logos consisting of thin outlines are ideal.

The cash register interface can now also print text and logos on the terminal's printer. See [9] for more information.

5.4 Related processing

5.4.1 Terminal Preparations

Before a terminal can be used by a merchant, it needs to receive its configuration. This activation process is described in 5.3.1.

Most of the configuration parameters the terminal will receive are created and filled in by TMS. However there are a few properties that TMS has no knowledge of and therefore need to be set by the distributor. Without correct values for these properties the terminal may not work properly after activation:

Domain	Name	Description
system	ntp.host	Host used by terminal to retrieve time information
modem	apn.name	Name of the APN to use for GPRS communication
modem	apn.user	APN username to use for GPRS communication
modem	apn.pass	APN password to use for GPRS communication
rdm	bos.url	URL of TMS
tdr	bos.url	URL to upload TDRs to
softwareupdate	download.url	URL where to look for software updates
pact2.ctap	terminalAccesProvider	Identifier for network provider 20404 = Vodafone

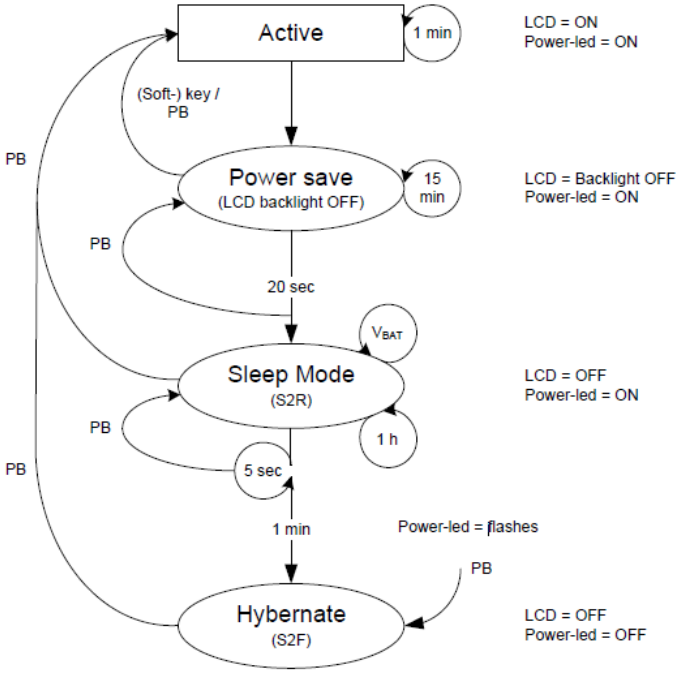
By default the following properties are set:

Name	Value
ntp.host	p4yntp
bos.url	https://p4ytms:8443/rdm/services/restv1/rdm/
download.url	p4ytms:8443/rdm/services/restv1/su

How to set these properties is detailed in the TMS SUM.

5.4.2 Low power modes

The terminal has an advanced power management scheme implemented, which is fully configurable by the user.



5.4.2.1 Power Save mode

While in the main menu and not being used for 60 seconds (configurable by the property gui:StatusPowerSaveTime), the terminal will go in power save mode. In this mode a message is displayed on screen and the display backlight is turned off.
The user can leave this mode and return to the main menu by pressing any key.
If the property gui:StatusPowerSaveTime is set to 0, the power save mode is disabled.

5.4.2.2 Low Power mode

If the terminal has been in Power Save mode for the time configured in gui:StatusLowPowerMode, then the terminal will switch to Low Power mode. In Low Power mode the terminal enters the 'suspend to RAM' state. Pressing the power button on the side of the terminal instructs the terminal to leave the Low Power mode. The terminal will return to the main menu.

The terminal supports two different Low Power modes, configurable by the property system:LowPowerMode.
The default value is 'normal' and in this mode the terminal suspends to RAM, but periodically wakes up to check the battery. This period is configurable by the property system:LowPowerBatteryCheckPeriod. If the battery drops below the threshold configured by the system:LowPowerEmtpyBatteryVoltage property, or the terminal has been in low power mode for longer than the time configured in system:AutoSuspendTime, then the terminal will go into hibernate.

The second low power mode is activated when the system:LowPowerMode is set to 'ultra'. In this mode the terminal consumes even less battery then in normal low power, but there is no periodic battery check or auto suspend (to flash) functionality.

5.4.2.3 Hibernate

When the terminal hibernates it writes its current state to flash and then completely shuts down. This state is therefore also referred to as suspend to flash. Storing the current state takes some time,

during which the terminal in non-responsive to key presses. This is indicated by the flashing power led.

At this point the terminal will not use any battery. Turn the terminal back on by pressing the power button.

5.4.3 Remote management sessions

The terminal is remotely manageable by the Terminal Management System (TMS). TMS can read and update properties on the terminal and trigger the terminal to perform certain requests. These requests can be any of

- Send log file
- Send complete properties description
- Send complete current state
- Perform a software update

There are two ways a management session can be started. The first is to use the menu. Go to 'TECHNISCH MENU' -> 'UPDATE' and the select 'YES'. A management session is started immediately.

The second way is by means of keep-alive messages. The terminal periodically sends a keep-alive message to TMS. This happens in the background and no user action is required. A keep-alive simply asks the TMS whether there are any messages (notifications and/or property updates) for this terminal. If so, TMS will respond this to the terminal. It is then up to the terminal to perform a management session. This session will then also run in the background.

The keep-alive interval is configurable and default set to 900sec. (rdm:keep.alive.interval).

If a keep-alive was scheduled, but could not be executed at the scheduled time (e.g. because a payment was being performed at that time), then the keep-alive will be rescheduled after 60 seconds, instead of the configured interval. This is to prevent missed management calls if TMS has some information for the terminal.

See TMS SUM on description how to configure properties for a device in TMS.

5.4.4 Transaction Data Records (TDR)

After each transaction a TDR is stored for transmission to TMS. A TDR contains summary data about the transaction. Storing them in TMS allows merchants to view the transactions performed with their terminals via a web interface. See TMS SUM for more info on this.

The TDRs are also used to convey the e-journals. E-journals contain more information that TDRs, but the mechanism is the same. TDR functionality is, unlike e-journal, non-configurable and always enabled.
If TDR's cannot be send to the TMS they are stored on the terminal. The maximum amount of TDR's that can be stored is configurable via the parameter tdr:max.allowed.tdr and is default set to 250. When TDRs can be sent again, they will be sent in batches. The size of these batches are configurable via the parameter tdr:tdr.batch.size and is default set to 10.

5.4.5 Software update

The terminal software architecture defines two different virtual machines (VMs). One is the 'live VM' for normal operation of the terminal. The other is the 'update VM' that takes care of the software update process. The software in the update VM can itself be updated. See [4] for a description of the software download design.

Each delivery of the Terminal Application software contains two feed directories, one for the live VM and one for the update VM. These feeds contain the software updates packages and are placed on a software download server.

A software download can be scheduled for a terminal via TMS. When the terminal receives the software update from TMS, it will wait until all these preconditions are fulfilled:

- External power is connected
- Network interface is available
- Terminal is idle

As soon as this is the case, the terminal will start the software update process. This process can't be cancelled by the user. After a power cycle, the software update process will resume. The software update process must run until completion before payment functionality (and normal operation mode) becomes available again.

The software update process consists of 6 steps. The terminal displays the currently executing step on screen. It is normal that during the software update process the terminal performs one or more reboots.
The terminal will automatically return to the main menu after the software update process has completed.

Depending on the value of the property 'softwareupdate:software.update.report.enabled', a receipt may be printed after the software update has completed. This receipt provides the user with feedback about the fact that the terminal software was just updated. The printed text can be configured with the parameter softwareupdate:software.update.report.text.

5.4.6 Network switching

5.4.6.1 Introduction

Since terminal software version 3.2 the terminal is able to dynamically switch between the Ethernet and the GPRS network. Switching to Ethernet only take a few seconds while switching to GPRS will take up to 45 seconds. A distinction is made between:

- Preferred network interface.
- Backup network interface.
- Active network interface.

The *preferred* network interface is the network interface that is used in normal situations. The terminal reports the set preferred network interface to the acquirer during a transaction regardless which network is actually active. The preferred network interface can be set during activation of the terminal or via the "Technical Menu -> Technical Settings -> Select Network" menu.

The *backup* network interface is the network interface that is used when the preferred network interface has no connection. This is not a setting since the backup network interface is the network interface that is not the preferred one.

The *active* network interface is the network interface that is currently being used. The active network interface can be selected manually via the "Settings -> Switch Network" menu. Or when configured in TMS the active network interface can also be changed automatically when the *preferred* interface cannot make a connection. Changing the active network interface is temporary. When the terminal is restarted it will start making a connection using the *preferred* network interface.

A typical scenario for this feature is that the terminal is normally fixed (preferred network Ethernet) and that sometimes the terminal is taken outside for a payment over GPRS. The terminal can then automatically switch to GPRS.

Or the terminal can automatically switch to GPRS when there is a problem with the fixed Internet connection. Here the GPRS is only used as backup when fixed Internet is temporary down.

Software updates are done via the preferred network. Thus in the situation where the terminal is used via GPRS but at night is attached to Ethernet for TMS/software update sessions, the terminal

must be set to Ethernet as preferred connection with automatic switching to backup. The terminal will then use GPRS when no network cable is attached and via Ethernet when a cable is attached.

5.4.6.2 Network switching modes

The active network interface can be switched manually (via the “Settings -> Switch Network” menu) or automatically when the *preferred* network interface cannot make a connection or when the connection of the preferred network interface is restored.

The mode of switching is determined by the “network/SwitchingMode” TMS parameter. It possible values are:

SwitchingMode	Description
0	No network switching at all (network switching menus also disabled).
1	Only manual network switching via the menus (similar to terminal software 3.1 and lower).
2	Automatic network switching in both directions with asking the user for confirmation. Confirmation is required for both switching from the *preferred* to the *backup* network interface and when switching from the *backup* to the *preferred* network interface.
3	Automatic network switching with asking the user for confirmation in backup direction only. Confirmation is required only for switching from the *preferred* to the *backup* network interface. Switching back from the backup network interface to the *preferred* network interface happens without confirmation.
4	Automatic network switching in both directions without asking the user for confirmation.

When allowed by the switching mode, the terminal will automatically switch from the *preferred* network interface to the *backup* network interface when it detects connection problems. When the backup connection is active, the status line will show a message that the backup connection is currently used. When the backup connection is also down, the status line will display a message that there is not backup connection. It will only switch back automatically to the *preferred* connection when the *preferred* connection is up again.

When the network connection is lost and automatic switching is disabled or when the user does not give permission to switch, the status line will show a message indicating there is a network problem. In that case the user can then later manually switch the network via the settings menu (only when the switching mode is 1 or higher).

5.4.6.3 Lost connection detection

There are two mechanisms that are used to detect if a network connection is down. The first is checking if the physical interface is connected to a network. This can detect if for example the Ethernet cable is disconnected/reconnected or if a SIM card is removed/inserted.

But the first mechanism does not detect if there is a problem further in the network. For example when the connection with a local router is good but the router does not have an internet connection. To detect these connection problems, the terminal can check if it can connect to certain hosts. Periodically the terminal will try to connect the hosts on the host list. When all hosts on the list are not reachable, the terminal assumes there is no internet connection and when allowed will switch to the backup network interface.
When one or more hosts on the list are reachable then the terminal assumes there is an internet connection and won’t switch. When the physical connection is up but all the hosts are not reachable, the status line will show “NO INTERNET” as message.

The behaviour of the “host checker” is determined by the “network:HostChecker.xxx” TMS parameters. The “network:HostChecker.Hosts” parameter contains a semi-colon separated list with hosts to check. A host entry is a URL in the form:

<protocol>://<host>:<port>

When no port number is given, the port will be derived from the protocol. When no protocol is given a port number must be provided. The port number will override the standard port number for the protocol. A list with valid URLs is for example:
http://www.chess-pt.com;http://www.google.nl:80;www.amazon.com:80

Choose for the hosts two or three servers that are likely to be up nearly always like Google. Specifying only one host is not a good idea because then a problem with that one host will result in a network switch while the Internet was still reachable. This can be prevented by having more hosts as it is unlikely that two or more host will be down at the same time.

The hosts in the list are checked right after each other. But before the list is processed again, the terminal will wait. This waiting time is determined by the “network:HostChecker.Interval” parameter. Its value is in seconds.

When the terminal switched to the *backup* network interface because the hosts were unreachable, it can’t check if the hosts are reachable again via the *preferred* network interface. To check if the hosts are available via the *preferred* network interface, the terminal has to switch back to the *preferred* network interface and try again.
There are two parameters that determine the time after which the terminal switches back to the *preferred* network interface when the switch to the *backup* interface was due to unreachable hosts (no internet) namely “network:HostChecker.SwitchBackTime” and “network:HostChecker.SwitchBackTimeHostsUnreachable”. These parameters contain the time after which to switch back in seconds. The first one is used when the hosts are reachable via the *backup* network interface and thus switching back is not urgent. The second one is used when the hosts are also not reachable via the backup network interface and switching back earlier to check the preferred network is desirable. Thus usually the value of *SwitchBackTime* is much bigger than the *SwitchBackTimeHostsUnreachable* value.

NOTE: The parameters related to the host checker are cached to minimise performance impact. This means that updates to these parameters via TMS will only be used when the terminal is rebooted.

5.5 Data backup

If the configuration of the terminal was somehow corrupted, it is possible to restore the factory default settings, see 5.3.2.5.8.1.

5.6 Recovery from errors, malfunctions, and emergencies

The terminal can be powered off abruptly In the event the terminal is no longer responding or otherwise misbehaving. Press and hold the power button for five seconds. The power led will go off and the terminal is shut down. Note that this procedure may cause damage to the terminal and should be used with care.

NB: when the terminal is powered on again, the boot sequence will take longer than normal.

When a cold restart does not solve the issue, as a last resort the terminal can be swept clean, see 0. A clean sweep destroys all information stored on the terminal, including activation and payment data.

5.7 Messages and error codes

5.7.1 C-TAP result codes

The C-TAP result code will be reported in the terminal log file as the payment result.

Code	Description
0	CTAP_RSLT_OK
1	CTAP_RSLT_ERROR
2	CTAP_RSLT_REMOVE_FROM_LIST
3	CTAP_RSLT_NEED_INSTALL
4	CTAP_RSLT_NEED_SIGN_ON
5	CTAP_RSLT_NEED_SIGN_OFF
6	CTAP_RSLT_NEED_COLLECTION
7	CTAP_RSLT_NEED_MANAGEMENT
8	CTAP_RSLT_BLOCKED
9	CTAP_RSLT_INVALID_TYPE
10	CTAP_RSLT_INVALID_AMOUNT
11	CTAP_RSLT_INVALID_CURRENCY
12	CTAP_RSLT_PARAMETER_INVALID
13	CTAP_RSLT_OPTION_NOT_SUPPORTED
15	CTAP_RSLT_NEED_DEINSTALL
20	CTAP_RSLT_SECURITY_PROBLEM
21	CTAP_RSLT_NO_CONNECTION
22	CTAP_RSLT_DATACOM_PROBLEM
23	CTAP_RSLT_CUSTOMER_ABORTED
24	CTAP_RSLT_MERCHANT_ABORTED
25	CTAP_RSLT_CARD_REMOVED
26	CTAP_RSLT_CARD_NOT_SUPPORTED
27	CTAP_RSLT_CARD_INVALID
28	CTAP_RSLT_CARD_PROBLEM
29	CTAP_RSLT_BALANCE_TOO_LOW
30	CTAP_RSLT_REFUSED_BY_HOST
31	CTAP_RSLT_NEED_VOICE_AUTH
40	CTAP_RSLT_NOT_IDLE

5.7.2 Transaction Host Incident Codes

The Transaction Host Incident Code is the code that is returned by the payment host as part of the authorization response, in reply to an authorization request from the terminal. In short, a value not equal to '0000' means the transaction has failed.

Code	Description
0000	Command message accepted.
1001	Balance request rejected; no support for 'site'.
1002	Balance request rejected; no support for closing terminal.
1003	There are still open/unconfirmed transactions for this terminal.
1004	Authorisation problem.
1005	Original transaction cannot be found.
1006	Cancellation not allowed.
1007	Cancellation amount not equal to the original amount.
1008	Certification code error.
1009	MAC error.

Source: ops.terminalspecificaties@nl.equens.com

5.7.3 Transaction Result Codes

Below, the transaction result codes that can appear on the terminal display, and/or on the receipt are listed. The codes below are used by Equens and can be different when another acquirer is used

Host incidentcode	Description
0000	Transactie akkooord
0120	opvragen counters voor site niet toegestaan
0120	Afsluiten door merchant niet toegestaan
0120	Er is nog een openstaande transactie
0100	Niet geaccepteerd
0101	Kaart geexpireerd
0103	Contact opnemen met de acquirer
0104	Kaart met beperkte mogelijkheden
0107	Doorverwijzen naar kaart-issuer
0109	Merchant niet bekend
0110	Bedrag niet toegestaan
0111	Ongeldig kaartnummer
0120	Transactie niet toegestaan op terminal
0121	Bedrag overschreden
0123	Transactielimiet overschreden
0124	Ongeldige currency
0902	Ongeldige transactie
0904	Formaat fout
0907	Issuer down
0911	Timeout bij aanvragen autorisatie
0912	Issuer niet bereikbaar
0913	Dubbele transactie
0914	Oorspronkelijke transactie niet gevonden
0916	MAC fout
0931	Cancellation niet toegestaan
0401	Bedrag cancellation niet gelijk aan oorspronkelijke transactie
0197	Terminal certificering probleem

5.7.4 Download Result Codes

When a parameter download, balance request or scheme load request fails, respectively the screen “download mislukt, code <x>”, “download tellers mislukt, code <x> or “keyload mislukt, code <x>” is shown. The possible codes that can occur for <x> are listed below.

Code	Description
01	General error.
06	Collection needed.
08	Acquirer was blocked.
13	Mandatory parameter was not set.
20	Security problem.
21	No connection.
22	Data transport problem.
23	Customer aborted.
24	Merchant aborted.

5.7.5 06 codes

Code	Description
0	LERT_NO_ERROR
1	LERT_SECURITY_ERROR
2	LERT_HOSTCOMM_ERROR
3	LERT_INT_HW_ERROR
4	LERT_INT_SW_ERROR
5	LERT_TIMEOUT_CUST
6	LERT_CUST_STOP
7	LERT_TIMEOUT_MERCHANT
8	LERT_MERCHANT_STOP
9	LERT_RECEIPT_PRINTER_ERROR
10	LERT_JOURNAL_PRINTER_ERROR
11	LERT_ELECTR_JOURNAL_ERROR
12	LERT_MAGSTRIPE_ERROR
13	LERT_ICC_ERROR
14	LERT_CUSTOMER_UI_ERROR
15	LERT_MERCHANT_UI_ERROR
16	LERT_TERMINAL_PARAMS_ERROR
17	LERT_TRX_TYPE_NOT_SUPPORTED
18	LERT_AMOUNT_NOT_SUPPORTED

5.7.6 Transaction Terminal Treatment Result codes

The transaction terminal treatment result field shall be transmitted by the terminal in the completion advice. It is used to inform then acquirer about the result of the transaction at the terminal side. Its main aim is to make the distinction between the positive completion advice and the negative completion advice. In the last case, it is used to inform the acquirer about the reason of the cancellation.

The possible codes are defined below. They also appear on the transaction journals/transaction detail records. The descriptions that contain '(should not occur)' are for cases that the Pay4You Terminal does not (yet) support. However, they have been listed for completeness.

Code	Description
0000	Positive advice.
1802	Unexpected message.
1803	Time-out expiration.
1804	Rejection notification.
1811	Technical problem.
1822	Connection failure.
1823	Invalid response.
2620	Card-required advice.
2621	Cancellation on PIN entry.
2622	Time-out on PIN entry.
2623	Card refusal.
2624	Card rejection.
2625	Corrupted response.
2626	Data authentication failure.
2627	Host refusal.

2628	Magnetic stripe fallback not allowed.
2629	Cancellation.
2707	PIN try exhaustion.
3000	CSM communication failure (no or invalid response).
3001	CSM internal error (SW12 error returned).
3313	MAC verification failure.
5503	Terminal reset, power failure.
2630	Denial after referral (should not occur).
2632	Cancelled transaction (should not occur).
2634	Data inconsistency (should not occur).
7000	Problems interfacing the external device in charge of goods delivery or service accomplishment (should not occur).
7006	Unexpected transfer of responsibility (should not occur).
7100	Time-out waiting for the use of the dispenser (should not occur).
7200	Operation result with financial amount equal to zero and with volume, if any, equal to zero (should not occur).
7300	Operation result with financial amount equal to zero but with volume greater than zero (should not occur).
7500	Unexpected operation result (should not occur).
7600	Transaction lost (should not occur).
7800	Data conversion problems (should not occur).
9002	Wrong product (should not occur).
Others	Reserved.

5.8 Quick-reference guide

Refer to [3] for the (quick) user guide of the Pay4You terminal.

6 Notes

Empty for this release!

7 Annexes

7.1 Pay4You Terminal Properties

For the types, the following values exist:

- **RO:** The property is read-only; Is set by the terminal
- **S:** The property is a terminal setting, and can be modified by a user;
- **P:** The property is a terminal parameter, changing it may influence the terminal's behavior;
- **I:** The property is an internal terminal property and should not be modified.

For the responsible parties, the following values exist:

- **T:** The terminal itself is responsible for this property;
- **EX:** An external party (e.g. the user) is responsible for this property;
- **TM:** The Terminal Manager is responsible for this property;
- **TMS:** The Terminal Management system is responsible for this property.

7.1.1 Domain "pact2"

Name	Description	Type	Resp.
keypad.controller.serial.number	Serial number of the keypad controller	RO	T
lcdpca.serial.number	Serial number of the LCD PCA	RO	T
pact2live.version	Version number of currently loaded terminal software.	RO	T
powerio.serial.number	Serial number of the PowerIO PCA	RO	T
terminal.product.id	The product id of the terminal	RO	T
terminal.serial.number	The terminal specific serial number.	RO	T
domain	Used to verify if this terminal may connect to a specific TMS.	P	EX

7.1.2 Domain "gui"

Name	Description	Type	Resp.	Default
AllowedMerchantLanguages	Defines the languages the user can select in the language menu, must be a subset of the installed languages	S	EX	nl_NL:NEDERLANDS
CashRegister.ConnectionString	The connection string for connection to a cash register.	S	EX	TCP;CashRegister:10000
CashRegister.KeepAliveInterval	The interval used for sending keep-alive messages to the cash register (can be overridden by the cash register).	S	EX	10
CashRegister.Message	The message shown on the terminal when it is waiting for a command from the cash register.	S	EX	WELKOM\nwacht op bedrag
CashRegister.Status	The state of the cash register interface (disabled (0), enabled (1), active (2))	I	T	0
CTAPManagerSettings	Needed for interaction between GUI and C-TAP application.	S	T	120_{hex}
ContactProvider	The message to display when provider contact is required	S	EX	NEEM CONTACT OP MET SERVICE PROVIDER
DisplayContrast	The current display contrast of the terminal. The value may be any positive integer from the range [170,175, 180, ..., 230]. Modifiable from terminal as well.	S	EX	210
DisplayLight	Whether the terminal display backlight is on.	S	EX	1

	A value of '1' means 'on', '0'means 'off'. Modifiable from terminal as well.			
EmptyBatteryVoltage	The voltage indicating an empty battery. In milliVolts.	P	T	7200
FullBatteryVoltage	The voltage indicating a full battery. Should only be changed to fine-tune terminal behaviour. In milliVolts.	P	T	8100
KeypadLight	Whether the terminal keypad backlight is on. A value of '1' means 'on', '0'means 'off'. Modifiable from terminal as well.	S	EX	0
LowBatteryVoltage	The voltage indicating a low battery. Should only be changed to fine-tune terminal behaviour. In milliVolts.	P	T	7250
MerchantLocale	The default merchant locale used to determine the language in the GUI. Currently supported locales are 'nl_NL', 'en_US', 'de_DE' and 'fr_FR'.	S	EX	nl_NL
MinimalModemSignalStrength	The minimal modem signal strength required for a transaction.	P	T	0
MuPadMessage	Default text when MuPad is connected	S	EX	WELKOM
MuPadStatus	Reflects whether the mupad is activated or not.	RO	T	1
NetworkInterface	The network interface the terminal currently uses. Possible values are 'Ethernet' and 'GPRS'. Modifiable from terminal as well.	S	EX	GPRS
Password	The password for the 'Technical Settings Menu' and 'C-TAP Menu'. Modifiable from terminal as well.	S	EX	2009
PaymentBlocked	Indicates whether payment functionality is blocked or not. Can only be set on terminal, must be cleared through TMS.	S	EX	0
PaymentBlockedMessage	The message to display when a payment is attempted, while payment functionality is currently blocked.	S	EX	NEEM CONTACT OP MET SERVICE PROVIDER
paymentReferenceEnabled	Whether payment reference is enabled or not. A value of '1' means 'enabled, '0' means 'disabled'. Modifiable from terminal as well.	S	EX	0
PaymentReferencePrefix	Text printed before payment references	S	EX	BetaalKenmerk_
RoasUrlList	A list of URLs and description of ROAS applications that will be shown in the "ADDED FUNCT." menu.	S	EX	
RoasUrlPaymentBlocked	A URL to the ROAS application that will be executed when a payment is blocked.	S	EX	
RoasUrlPaymentEnd	A URL to the ROAS application that will be executed when a payment has finished.	S	EX	
RoasUrlPaymentFailed	A URL to the ROAS application that will be executed when a payment has failed.	S	EX	
RoasUrlPaymentStart	A URL to the ROAS application that will be executed when a payment is started.	S	EX	
RoasUrlResume	A URL to the ROAS application that will be executed when the terminal resumed from suspend to flash.	S	EX	
RoasUrlSoftwareUpdateEnd	A URL to the ROAS application that will be executed when a software update has finished.	S	EX	
RoasUrlSoftwareUpdateStart	A URL to the ROAS application that will be executed when a software update is started.	S	EX	
RoasUrlStartUp	A URL to the ROAS application that will be executed when the terminal starts up (cold boot).	S	EX	
RoasUrlStateIdle	A URL to the ROAS application that will be executed when the terminal receives a "execute ROAS application" request from	S	EX	

	TMS.			
ServicePassword	The password for the 'Service Menu'. Not modifiable from the terminal	P	EX	5820
StatusLowPowerTime	Time in seconds after which the terminal enters 'low power' mode	S	T/EX	900
StatusPowerSaveTime	Time in seconds after which the terminal enters 'power save' mode.	S	T/EX	60
StatusRefreshTime	Period in seconds with which GUI updates its status (network, battery, printer, etc.).	P	T	5
TerminalActivated	Whether the terminal has been activated or not. A value of '1' means 'activated, '0' means 'not yet activated'.	RO	T	0

7.1.3 Domain "rdm"

Name	Description	Type	Resp.	Default
bos.url	Host name of the TMS RDM interface.	S	EX	https://p4ytms:8443/rdm/services/restv1/rdm/
connection.timeout	Number of seconds after an RDM connection attempt times out.	S	EX	300
device.type	The name of the terminal model.	P	T	PACT2
keep.alive.interval	Number of seconds between keep-alive messages.	S	EX	900
logical.id	The terminal's logical ID.	P	TM	0
protocol.timeout	Number of seconds after an active RDM connection times out.	S	EX	300
set.current.time	This defines whether the terminal will synchronize its clock with TMS after the next RDM message exchange. A value of '1' means 'synchronize', '0' means 'do not synchronize'.	S	EX	1

7.1.4 Domain "system"

Name	Description	Type	Resp.	Default
AutoSuspendTime	Time in minutes before the terminal goes to hibernate	S	EX	60
EmptyBatteryHysteresis	If battery level is less than 'LowPowerEmptyBatteryVoltage + EmptyBatteryHysteresis', the terminal will not boot	S	EX	100
LowPowerBatteryCheckPeriod	Period in seconds to check for empty battery while in low power mode	S	EX	60
LowPowerEmptyBatteryVoltage	If the battery voltage drops below this value while in low power mode, the terminal goes to hibernate	S	EX	7250
LowPowerMode	The type of low power mode to use. Possible values are 'normal' and 'ultra'	S	EX	normal
ntp.host	Host name of the terminal's NTP server.	S	EX	p4yntp
ntp.port	Port number of the terminal's NTP server.	S	EX	0
RebootReason	The reason of the last reboot (none (0), cold start (1), warm start (2), software update (3)).	I	I	

7.1.5 Domain “modem”

Name	Description	Type	Resp.	Default
apn.name	Name of the GPRS access point.	S	EX	<empty>
apn.user	Username for GPRS connections.	S	EX	<empty>
apn.pass	Password for GPRS username ‘apn.user’.	S	EX	<empty>
simid	The ID of the inserted SIM card	RO	T	<empty>

7.1.6 Domain “tdr”

Name	Description	Type	Resp.	Default
bos.url	Host name of the TMS TDR interface.	S	TM	https://p4ytms:8443/rdm/services/restv1/tdr/
connection.timeout	Number of seconds after a TMS connection attempt times out.	S	EX	30
max.allowed.tdrs	The maximum amount of TDRs the terminal can hold.	S	EX	250
protocol.timeout	Number of seconds after an active TMS connection times out.	S	EX	30
tdr.batch.size	Specifies the maximum amount of TDR send during a TDR upload.	P	TM	10

7.1.7 Domain “softwareupdate”

Name	Description	Type	Resp.	Default
download.url	The host name of the TMS software-download interface (without http(s):// prefix).	S	EX	p4ytms:8443/rdm/services/restv1/su
SB.started	Internal property required for software update.	I	T	1
software.update.state	The terminal’s current software-update state. Can be one of: ‘idle’, ‘pending’, ‘started’, ‘updating’, ‘updated’.	I	T	idle
software.update.report.enabled	Specifies whether a report is printed at the end of the software update.	S	EX	0
software.update.report.text	When the report is enabled, the property specifies the text to be printed at the report.	S	EX	SOFTWARE UPDATE COMPLETE

7.1.8 Domain “tms”

Property values in the TMS domain are created and maintained by TMS. The terminal has no knowledge or influence on them. They are listed here solely for completeness of the property listing.

Name	Description	Type	Resp.
mgtsession.last-successful	Time in UTC of last successful management session.	I	TMS
mgtsession.keepalive.time	Time in UTC of last keep-alive message.	I	TMS
mgtsession.starttime	Time in UTC of last management session.	I	TMS
sw.update.starttime	Time in UTC of start of software update session.	I	TMS

7.1.9 Domain “st”

Name	Description	Type	Resp.	Default
enter.pin.ch14.<x>	PIN entry screen ch14 (language <x>).	S	TM	See [5], §4.1.5
enter.pin.ch216.<x>	PIN entry screen ch216 (language <x>).	S	TM	See [5], §4.1.5
incorrect.pin.ch217.<x>	Incorrect PIN entered screen ch217 (language <x>).	S	TM	See [5], §4.1.5
incorrect.pin.ch218.<x>	Incorrect PIN entered screen ch218 (language <x>).	S	TM	See [5], §4.1.5
request.tip	Tip request screen (obsolete, replaced by request.tip.<x>).	S	TM	See [5], §4.1.5
request.tip.<x>	Tip request screen (language <x>).	S	TM	See [5], §4.1.5

7.1.10 Domain “ts”

Name	Description	Type	Resp.	Default
enter.pin.ch14.<x>	Signature over PIN entry screen ch14 (language <x>).	S	TM	<binary>
enter.pin.ch216.<x>	Signature over PIN entry screen ch216 (language <x>).	S	TM	<binary>
incorrect.pin.ch217.<x>	Signature over Incorrect PIN entered screen ch217 (language <x>).	S	TM	<binary>
incorrect.pin.ch218.<x>	Signature over Incorrect PIN entered screen ch218 (language <x>).	S	TM	<binary>
request.tip	Signature over tip request screen (obsolete, replaced by request.tip.<x>).	S	TM	<binary>
request.tip.<x>	Signature over tip request screen (language <x>).	S	TM	<binary>

7.1.11 Domain “pact2.ctap”

Name	Description	Type	Resp.	Default
<ACQID>_<CTRID>.FC	Financial counter related properties for financial counter with acquirer id <ACQID> and counter id <CTRID>. Represented as TLV structure.	I	T	<binary>
<ACQID>_<CBID>.SF	Shift related properties for shift with acquirer id <ACQID> and card brand id <CBID>. Represented as TLV structure.	I	T	<binary>
<ID>.AC	Acquirer related properties for acquirer with id <ID>. Represented as TLV structure.	S	TM	<binary>
<ID>.AP	Saved acquirer-parameter message for acquirer with id <ID>. Represented as TLV structure.	I	T	<binary>
<ID>.CB	Card brand related properties for card brand with id <ID>. Represented as TLV structure.	S	TM	<binary>
<ID>.SE	Security scheme related properties for Security scheme with id <ID>. Represented as TLV structure.	S	TM	<binary>

<ID>.TR	Saved completion advice message for acquirer with id <ID>. Represented as TLV structure.	I	T	<binary>
acquirerData<x> (0 <= x < 10)	Terminal's internal acquirer specific data, for acquirer with id <x>.	I	T	<binary>
addNonMandatoryTags	defines whether we add non-mandatory tags to authorization request and completion advice messages. E.g. the TSI_TAG is not mandatory according to C-TAP specifications for both message types. However, for Cetecom EMV-L2 and VISA brand testing purposes, this tag's value has to be checked for correctness.	S	TM	0
blockedFlags	If this value does not equal '0', the terminal is blocked for payments.	I	T	0
capkParametersVersion	Version number of the currently loaded Certification Authority public keys.	S	TM	1
CAPKT	Represents the currently loaded C-TAP Authority public keys, as TLV structure.	S	TM	<binary>
certCode	The certification code as issued by the C-TAP Authority.	S	TM	0
commonParametersId	Version number of the currently loaded C-TAP common parameter set.	S	TM	1
configManagementReason	Indicates the reason why certain configuration management needs to be performed	I	T	0
CTACM	Represents the currently loaded set of acquirers, as TLV structure.	S	TM	<binary>
CTAID	Represents the currently loaded Application Identifier table, as TLV structure.	S	TM	<binary>
CTBIN	Represents the currently loaded BIN table, as TLV structure.	S	TM	<binary>
CTCBM	Represents the currently loaded set of card brands, as TLV structure.	S	TM	<binary>
CTMPT	Represents the currently loaded Magstripe Protection Table, as TLV structure.	S	TM	<binary>
currencycode	The currency code supported by the terminal.	S	TM	978_{bcd}
currentTscManId	Manufacturer ID of the current TSC.	RO	T	0
currentTscSerialNr	Serial number of the current TSC.	RO	T	00000000
currentTscSoftVersion	Version number of the currently used TSC software.	RO	T	0
dateForUpdate	Timestamp after which a management session has to be done. Otherwise, terminal will be blocked for payment. Value is in seconds since 1970.	S	TM	<time of first boot>
eJournalEnabled	Whether an electronic journal is kept.	S	EX	0
emvKernelChecksum	Checksum calculated over EMV Kernel software.	RO	T	<empty>
enabledServices	Indicates the allowed services for the terminal. See C-TAP.220 2.12.12 for possible values.	S	TM	$FFFFFF_{hex}$

endBusinessHours	Represents the end business hours, per day of the week. Value is displayed as 'xxxxxxxxxxxxxx', e.g. '20202020202020' for end hour of 10PM each day.	S	EX	<binary>
extDeviceInUse<x> (0 <= x < 4)	Whether external device <x> is in use or not. '1' means 'in use', '0' means 'not in use'.	S	EX	0
extDeviceName<x> (0 <= x < 4)	The name of external device <x>.	S	EX	<empty>
extDeviceType<x> (0 <= x < 4)	The type of external device <x>. '0'means 'buiten gebruik', '1' means 'onbekend', '2' means 'kassa', '3' means 'automaat' and '4' means 'pomp'.	S	EX	0
extDeviceVersion<x> (0 <= x < 4)	Version number of external device <x>.	S	EX	0
ifdSerialNumber	The terminal serial number	S	TM	12345678
language	C-TAP user interface language.	S	EX	DUTCH
lastLoadedMPTVersion	Contains the version number of the currently loaded MPT.	RO	T	<empty>
lastOfflineDeclinedTxnData	Transaction Data of the last offline declined transaction. Required by EMV L2 specification for verification purpose	RO	T	<binary>
mac.acquirer.<ID>.AC	Backup of property <ID>.AC, for verification purposes.	I	T	<binary>
mac.cardbrandtable	Backup of card brand table, for verification purposes.	I	T	<binary>
mac.commonParams	Backup of the common parameters, for verification purpose	I	T	<binary>
mac.CTACM	Backup of the acquire table, for verification purpose	I	T	<binary>
maxTipAllowed	The maximum allowed tip as percentage of the transaction amount.	S	EX	99
merchantReferenceEnabled	Indicates whether the merchant reference is enabled or not. '1' means 'enabled', '0' means 'disabled'. Currently not supported.	S	EX	0
MsgSeqNrOfSecurityScheme<ID>	Sequence number for security scheme related messages for Security Scheme with id <ID>.	I	T	<acquirer dependent>
parameter.set.version	Indicates the version of the currently loaded set of C-TAP parameters.	RO	T	25
preferredEmvDate	Date from which the terminal's preferred mode shall be 'EMV'. In seconds since 1970.	S	EX	$7FFFFFFF_{hex}$
preferredMode	Represents the preferred card insertion method: '1' indicates 'track3', '2' indicates 'EMV'.	S	EX	1
prevTechParamDownloadDay	Not used.	I	T	0
printTxnJournal	Whether the journal should be printed or not. Printed if set to 1, skipped if set to 0. Only effective if eJournalEnabled is set to 1	S	EX	1
receiptFooter	The text that will be printed as receipt footer.	S	EX	<empty>
scheduleProcessManagementCall	Whether a management session is scheduled. A value of '1' means a session is scheduled, '0' otherwise.	I	T	0

shiftOpenDateTime	Timestamp when current shift was opened. In seconds since 1970.	I	T	<time of first boot>
SSMParameters	Represents the currently loaded security schemes, as TLV structure.	P	TM	<binary>
startBusinessHours	Represents the start business hours, per day of the week. Value is displayed as 'xxxxxxxxxxxxxx', e.g. '08080808080808' for start hour of 8AM each day.	S	EX	<binary>
terminalAccesProvider	The access provider for the terminal.	S	EX	0
terminalCountryCode	Indicates the country in which the transactions take place. A value of '528' indicates "The Netherlands". See [ISO 3166] for other countries.	S	TM	528
terminalManagerId	ID of the Pay4You Terminal manager.	S	TM	52800008
terminalManParametersId	Indicates the validity of the current Terminal Manager Parameters set. '0' means 'invalid', other values indicate 'valid'. The terminal will be blocked for payments while this value is invalid.	S	TM	1
terminalManufacturerId	ID of the Pay4You Terminal manufacturer.	S	TM	52800008
terminalModel	The model of the terminal	RO	T	Pay4You
terminalPhoneNr	The terminal's phone number.	S	EX	00000311825 94000
terminalType	Indicates the terminal type according to C-TAP protocol. Pay4You Terminal is type '21', means attended, online only terminal.	S	TM	21
tipEnabled	Indicates whether tip functionality is enabled or not.	S	EX	0

7.1.12 Domain "printer"

Name	Description	Type	Resp.	Default
GraphicalLogo.Enable	Enables (1) or disables (0) printing of a graphical logo on the card holder ticket	S	EX	0
GraphicalLogo.BitmapData	The description and the bitmap data to upload to the terminal. When bitmap data is uploaded, the parameter only contains the description.	S	EX	

7.1.13 Domain "network"

Name	Description	Type	Resp.	Default
SwitchingMode	Determines how the terminal may switch the active network interface. Possible values are: 0. No network switching at all (switch menus also disabled). 1. Only manual network switching via the menus (similar to terminal software 3.1 and lower). 2. Automatic network switching with confirmation in both directions. 3. Automatic network switching with confirmation only from preferred to backup network.	S	EX	1

	4. Automatic network switching without asking for confirmation.			
HostChecker.Hosts	Contains a list of hosts to check (semi-colon separated). When the terminal can't contact all the hosts on this list, the terminal will assume there is no internet connection.	S	EX	
HostChecker.Interval	The interval between two sessions of host checks (seconds).	S	EX	5
HostChecker.SwitchBackTime	The time to switch back to the preferred network if the switch to the backup network was due to unreachable hosts instead of no network connection (seconds). This time is used when the hosts are reachable via the backup interface.	S	EX	1800
HostChecker.SwitchBackTimeHostsUnreachable	The time to switch back to the preferred network if the switch to the backup network was due to unreachable hosts instead of no network connection (seconds). This time is used when the hosts are also NOT reachable via the backup interface.	S	EX	300